

ONE INTERNET, MANY WORLDS

By Joe Telafici

A couple of years ago I came to the conclusion that tracking country of origin or destination of a malware attack was a pointless exercise—useful only for marketing purposes—and had no real predictive or prescriptive value. This perception was engendered by a couple of fairly recent (at that time) occurrences:

- Mass-mailers, especially W32/SQLSlammer.worm, proved that you could infect basically the entire Internet in a matter of minutes.
- In an attempt to avoid attracting the attention of law enforcement officials, malware writers stopped including useful clues in malware about its origins.
- The primary motivation for malware at this time was ego: the more machines infected, the more fame.

Contrast this to the situation in the mid-1990s, when threats started in one part of the world and took weeks to reach other parts. Moreover, the threat was likely to contain strings or resources very clearly pointing to the country of origin, as well as to the intent of the author.

However, in 2002 through 2004, threats such as Klez, Bugbear, SQLSlammer, Blaster, Sobig, Nachi, MyDoom, Netsky, and Bagle were global phenomena that hit virtually the entire planet in the space of only a few minutes to a few hours. For a while, it seemed like the global dominance of Microsoft Windows as a platform, the explosion of broadband usage throughout the world, the ease of finding vulnerabilities, and the application of social-engineering techniques would ensure that no one connected to the Internet was safe for very long from any threat.

During this period of intense malware replication, a trend began that, frankly, the anti-virus community as a whole failed to notice in its early stages. We discussed this phenomenon in our previous edition, "The Future of Cybercrime."¹ During 2004, an explosion of malware creation occurred that was larger in scale, but smaller in breadth, than anything seen to date. Bots, password stealers, and other static malware began to appear at alarming rates. Unlike the replicating viruses that characterized the last flurry in what I call the "digital graffiti" stage of malware development, these threats almost never rose to a global level for a variety of reasons. The main reason was that malware authors were not interested in drawing the kind of attention that the large-scale virus writers of Netsky and Sasser attracted from the law enforcement community.

Whether as a side effect, symptom, or cause of this low-and-slow paradigm shift, for these reasons malware has become more regional or localized in nature during the last two to three years:

- Better social engineering is now required for seeding attempts and to lure people to drive-by sites, phishing sites, or hosted malware. To appear legitimate enough to fool wary computer users, the kinds of egregious typos made by nonnative speakers are too obvious today.
- More vulnerabilities are being found now in more obscure software, including in some localized software (such as Ichitaro, a word processing package popular in Japan) due to the increase in vulnerability bounties, both from security vendors and from attackers.
- Malware authors show increased interest in limiting the sources of attacks to countries where law enforcement is likely to be lax.
- Malware authors are fond of attacking niche markets, whether to exploit a particular resource or to avoid law enforcement.

You'll see a number of examples of these kinds of country-, language-, company-, or software-specific attacks in the articles comprising this issue.

Although we can't ignore the motivations of the malware authors in focusing attacks, this activity takes place in a global environment that is quite different from that of even a few years ago. Political, economic, and social forces shape everything and have contributed to a whole underground economy and market whose diversification, breadth, and scope are larger than ever before.

One of the most significant factors increasing the possibilities for attackers is the growth in global broadband penetration. With broadband computers connected full-time to the Internet, the opportunity to attack systems in real time and to use spare bandwidth capacity on compromised machines for further attacks is a resource too tempting to ignore. But broadband penetration varies widely across the globe, with estimates ranging from nearly 90 percent in South Korea, to about 50 percent in the United States, to significantly less in parts of the developing world.

The expansion and diversification of the role of computers in modern society likewise contribute to expanded opportunities for those seeking to capitalize on cybercrime. From staggering growth in cell phone usage (upwards of 20 percent annually, with more than three billion subscribers expected by 2010), to online banking usage, online gaming, and e-commerce in general, there are enough money, vectors, and targets to ensure that the unscrupulous have plenty to keep them busy. But this technological storm is proceeding at a different pace in different parts of the world. For example, mobile technology is well ahead of the rest of the world in Asia, while online banking is at its most robust in Brazil, and online gaming is a cottage industry in China.

To some degree, cybercrime is a natural extension of what is probably among the world's oldest professions: theft. But we can't ignore the economic realities in many parts of the world that make this an attractive option. Particularly in Eastern Europe, where technical skills were widely taught during the Cold War but economic opportunities are limited, and in Asia, where population growth has stretched strong economic performance to the limits, the motivation to engage in questionable or illegal behavior increases. As a former virus writer remarked to me once, "I had to do something to feed my family."

As a former virus writer remarked to me once, 'I had to do something to feed my family.'

And it may not merely be the criminals getting in on the act. As the recent and ongoing distributed denial-of-service attack on Estonia's infrastructure demonstrates, political "hacktivists" may have an increasing interest in the Internet

1 "Sage," April 2007. http://www.mcafee.com/us/threat_center/white_paper.html

as a battlefield or potential theater. Whether nation states or military organizations have a similar interest is an unknown, though likely, assumption.

Given the variety of roles, motivations, and advantages of today's cybercriminals, how our society reacts is crucial to the maintenance of law and order in the Wild West of the Internet. It has become increasingly clear that human society is far from homogenous in its preparedness for and reaction to cybercrime. Here at McAfee® Avert® Labs, we work with a variety of law enforcement agencies in countries all over the world, and it is apparent to us that the legislative, financial, and technical resources available to crime-fighters in different parts of the world can be like night and day. And because it is rare for an attack to start, travel through, and end in the same country, this impacts our ability to impede or stop malware authors and crackers even when it is dead obvious who is involved. This inability to coordinate internationally is one of the largest factors contributing to the low-risk environment that characterizes cybercrime today.

Political 'hacktivists' may have an increasing interest in the Internet as a battlefield or potential theater.

In the following pages, you will hear from some of the world's most talented researchers based in, or with close ties to, the country whose security situation they are describing. I hope that you find the articles educational,

informative, and thought provoking. Although every nation faces different challenges in today's interconnected personal and business world, you cannot avoid affecting and being affected by the situations next door and across the sea.



Joe Telfaci is Vice President of Operations for McAfee Avert Labs. He has management responsibility for researchers in 16 countries on

five continents. With more than 10 years of experience at Symantec, CyberMedia, Tripwire, and McAfee in both consumer and corporate security products, Telfaci is responsible for coordinating McAfee's response to global security threats, as well as the daily production of security content, customer support tools, and research into next-generation threats and technology. He has briefed Congress on technology issues, is quoted regularly in the press on virus- and spyware-related issues, and has been published in *Virus Bulletin*.

Telfaci is from New Jersey and, although he misses the New Jersey Devils, he gets better beer and coffee in McAfee's Beaverton, Oregon, office.

